NỘI DUNG

4.1 Mã hoá số liệu mức vật lý

4.2 Phát hiện lỗi và sữa sai

4.3 Nén số liệu

4.4 Mật mã hoá số liệu

Sửa lỗi

- Cách sửa lỗi thông thường là yêu cầu truyền lại khối dữ liệu bị lỗi
- Không thích hợp cho các ứng dụng trao đổi dữ liệu không dây
  - Xác suất lỗi cao, dẫn đến việc phải truyền lại nhiều
  - Thời gian trễ truyền lớn hơn nhiều thời gian truyền 1 khối dữ liệu
  - Cơ chế truyền lại là truyền lại khối dữ liệu bị lỗi và nhiều khối dữ liệu khác tiếp theo
- Cần thiết sửa lỗi dựa vào các dữ liệu nhận được

Cyclic Redundant Check (CRC)

- Các lỗi được phát hiện

–Tất cả các lỗi bit đơn

–Tất cả các lỗi kép nếu P(x) có ít nhất 3 toán hạng

– Một số lẻ lỗi bất kỳ nếu P(x) chứa 1 thừa số (x+1)

– Bất kỳ lỗi chùm nào mà chiều dài của chùm nhỏ hơn hoặc bằng chiều dài FCS (n=k)

–Hầu hết các lỗi chùm lớn hơn

- CRC là một trong những phương pháp thông dụng và hiệu quả nhất để phát hiện lỗi

Cyclic Redundant Check (CRC)

- 4 đa thức sinh được sử dụng rộng rãi
  - CRC-12 = $X^{12} + X^{11} + X^3 + X^2 + X + 1$
    - 12-bit FCS
    - Dùng để truyền chuỗi các ký tự có độ dài 6-bit
  - CRC-16 = $X^{16} + X^{15} + X^2 + 1$
    - 16-bit FCS
    - Dùng để truyền chuỗi các ký tự có độ dài 8-bit
    - USA
  - CRC-CCITT = $X^{16} + X^{12} + X^5 + 1$
    - Europe
  - CRC-32 = $X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$
    - 32-bit FCS
    - Point-point synchronous transmission, DVB-T…

Ví dụ

- Vậy F = 01110
- Dữ liệu được truyền là T= 10111010000**01110**

Ví dụ

- Thực hiện phép chia

$$
\begin{array}{l|l}
x^5 + x^4 + x^2 + 1 & \underline{x^9} + \underline{x^8} + \underline{x^6} + \underline{x^4} + \underline{x^2} + \underline{x} \\
 & x^{14} + x^{12} + x^8 + x^7 + x^5 \\
 & x^{14} + x^{13} + x^{11} + x^9 \\
 & x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^5 \\
 & x^{13} + x^{12} + x^{10} + x^8 \\
 & x^{11} + x^{10} + x^9 + x^7 + x^5 \\
 & x^{11} + x^{10} + x^8 + x^6 \\
 & x^9 + x^8 + x^7 + x^6 + x^5 \\
 & x^9 + x^8 + x^6 + x^4 \\
 & \quad x^7 + x^5 + x^4 \\
 & \quad x^7 + x^6 + x^4 + x^2 \\
 & \quad x^6 + x^5 + x^2 \\
 & \quad x^6 + x^5 + x^3 + x \\
 & \quad\quad x^3 + x^2 + x \quad = R(x)
\end{array}
$$

Ví dụ

- Dữ liệu cần truyền 1010001101 (k = 10) → Đa thức biểu diễn $X^9 + X^7 + X^3 + X^2 + 1$
- Cho đa thức sinh: $P(x) = X^5 + X^4 + X^2 + 1$ (n – k + 1 = 6 hay n – k = 5 hay n = 15)
- Dữ liệu D dịch trái 5 bit. $X^{n-k}\ D(x) = X^5\ D(x) = X^{14} + X^{12} + X^8 + X^7 + X^5$

Cyclic Redundant Check (CRC)

- Cách khác để xác định FCS là dùng đa thức
  - D = 110011 $\rightarrow$ D(x) = $X^5 + X^4 + X + 1$
  - P = 11001 $\rightarrow$ P(x) = $X^4 + X^3 + 1$

$$\frac{X^{n-k}D(X)}{P(X)} = Q(X) + \frac{R(X)}{P(X)}$$

$$T(X) = X^{n-k}D(X) + R(X)$$

Cyclic Redundant Check (CRC)

- Số chia P
  - Dài hơn 1 bit so với FCS mong muốn
  - Được chọn tùy thuộc vào loại lỗi mong muốn phát hiện
  - Yêu cầu tối thiểu: msb và lsb phải là 1
- Biểu diễn lỗi
  - Lỗi = nghịch đảo bit (i.e. xor của bit đó với 1)
    - T: frame được truyền
    - Tr: frame nhận được
    - E: error pattern với 1 tại những vị trí lỗi xảy ra
  - Nếu có lỗi xảy ra (E ≠0) thì bộ thu không phát hiện ra lỗi đó khi và chỉ khi Tr chia hết cho P, nghĩa là E chia hết cho P khó có khả năng xảy ra

Ví dụ

- Vậy suy ra F = 01110
- Từ đó suy ra T = 10100011010111110

Ví dụ

- Cho khối dữ liệu D = 1010001101 (10 bit)
- Số chia xác định trước P = 110101 (6 bit)
- Tìm FCS = ? , T = ?
- Giải:
  - Ta có k = 10
  - n – k + 1 = 6
  - Suy ra n = 6-1+10 = 15
  - Lấy 2^{n-k} D chia cho P
  - $2^{n-k}D = 2^5$ D = 101000110100000
  - Lấy kết quả trên chia cho P ta được thương là 1101010110 dư 01110

Cyclic Redundant Check (CRC)

- Xác định
  - Nếu lấy F = R thì $T = 2^{n-k}D + R$
  - Chia T cho P ta có

$$\frac{T}{P} = \frac{2^{n-k}D + R}{P} = \frac{2^{n-k}D}{P} + \frac{R}{P}$$

  - Suy ra $\frac{T}{P} = Q + \frac{R}{P} + \frac{R}{P}$
  - Mà phép cộng modulo 2 của một số với chính nó bằng 0
  - Vậy $\frac{T}{P} = Q + \frac{R + R}{P} = Q$

Cyclic Redundant Check (CRC)

- Xác định
  - T = frame có n bit cần truyền
  - D = khối dữ liệu k bit (message) (k bit đầu của T
  - F = (n-k) bit FSC (n-k) bit cuối của T
  - P = số chia được xác định trước gồm n-k +1 bit

$$T = 2^{n-k}D + F$$

- Giả sử

$$\frac{2^{n-k}D}{P} = Q + \frac{R}{P}$$

Cyclic Redundant Check (CRC)

- Số học modulo 2
  - Cộng hai số nhị phân (không nhớ)
  - Exclusive OR (XOR)

$$\begin{array}{r} 1111 \\ +1010 \\ \hline 0101 \end{array} \qquad \begin{array}{r} 1111 \\ -0101 \\ \hline 1010 \end{array} \qquad \begin{array}{r} 11001 \\ \times\ 11 \\ \hline 11001 \\ 11001 \\ \hline 101011 \end{array}$$

Cyclic Redundant Check (CRC)

- Nguyên lý
  - k bit message
  - Bên phát tạo ra chuỗi (n-k) bit FCS (Frame Check Sequence) sao cho frame gửi đi gồm n bit chia hết cho một số xác định trước
  - Bên thu chia frame nhận được cho cùng một số và nếu không có phần dư thì có khả năng không có lỗi